Home Office

Detention Services Order 04/2017

Surveillance Camera Systems

February 2018

This publication is available at www.gov.uk/government/collections/detention-service-orders

Any enquiries regarding this publication should be sent to us at DSOConsultation@homeoffice.gsi.gov.uk

Contents

Document Details

Process: The use of surveillance camera systems including the management and security of data.

Implementation Date: February 2018

Review Date: February 2020

Version: 1.0

Contains Mandatory Instructions

For Action: Home Office staff and suppliers operating in immigration removal centres, pre-departure accommodation and short-term holding facilities and escorting suppliers.

For Information: Home Office caseworkers

Author and Unit: Frances Hardy, Operational Support and Guidance Team

Owner: Alan Gibson, Head of Detention Operations

Contact Point: Frances Hardy

Processes Affected: The use of surveillance camera systems including the management and security of data.

Assumptions: Surveillance camera system operators will have a good knowledge of the legislation that applies to its use.

Notes:

Instruction

Introduction

1. This detention services order (DSO) provides guidance for all staff working in immigration removal centres (IRC), pre-departure accommodation (PDA) and short-term holding facilities (STHF), as well as escorting staff, on the use of surveillance cameras. References to “centre” in this document cover IRCs, STHFs and PDA.

2. A surveillance camera system is the overarching term for any system used for recording and retaining visual images for surveillance purposes and will include the following:

- A body worn camera (BWC) is a camera worn on the body in an overt capacity by a user for the primary purpose of recording video and audio material.

- A hand held camera (HHC) is a camera with limited or no security features used for recording video and audio material by hand.

- Closed circuit television (CCTV) is the use of overt video cameras to transmit images to a specific limited number of televisions on the same network or circuit, primarily used for surveillance and security purposes.

Policy

3. Surveillance camera systems are used to monitor and record activity within immigration removal centres and during escort for the safety and security of staff, detainees and the public. Recorded footage can help assure that the highest professional standards are being maintained by staff and provides evidence useful in the investigation of complaints and/or criminal investigations or procedures.

4. Use of surveillance cameras and data must be in accordance with all relevant legislation including Data Protection Act 1998[1] (DPA), the Regulation of Investigatory Powers Act 2000 (RIPA)[2] as set out in DSO 02/2015, the Freedom of Information Act 2000[3], the Human Rights Act 1998 and the Protection of Freedoms Act 2012[4], where applicable.

[1] http://www.legislation.gov.uk/ukpga/1998/29/contents

[2] http://www.legislation.gov.uk/ukpga/2000/23/contents

[3] http://www.legislation.gov.uk/ukpga/2000/36/contents

[4] http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

5. It is important that there is a clear basis for the recording, storage and analysis of any detainee's personal information, including responsibilities and obligations under the DPA. As the Home Office has overall responsibility for the control of this information it acts as the data controller and those operating the surveillance systems (private contractor, HM Prison and Probation Service and escort suppliers) act as data processors under the DPA.

6. The use of surveillance cameras and management of data should also show due regard to the Home Office surveillance camera code of practice[5] and comply with the Home Office personal information charter[6]. In addition when a centre supplier is considering the introduction of any new surveillance system, or reviewing the use of any existing surveillance systems in a centre, the centre supplier must complete a privacy impact assessment (ICO PIA guide here) to assess the impact of the system on people's privacy (whether detainee, staff or visitor). This should include consideration of whether its intended use has a lawful basis and is justified, necessary and proportionate.

Procedures

7. The Data Protection Act (principle 7) requires that data controllers have appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. The centre supplier, as data processor, must have a local policy on the use of surveillance camera systems, which must clearly justify the need for both video and audio recording (for example gathering evidence or complaints management). Any consideration of recording audio alongside video recording must have a higher level of justification than video recording alone. The privacy impact assessment and both of the Surveillance Camera Commissioners self assessment tools[7] on the code of practice and body worn video should be completed when developing or revising the centre's local policy and the results be provided to the local HOIE team on request. The final policy must be agreed by the local HOIE delivery manager, in consultation with the Detention and Escorting Services Security Team before implementation. In addition the local HOIE delivery manager must agree any substantive revisions to the centre's local policy. Any issues arising with approval of the local policy should be escalated to the Head of Detention Operations for a final decision.

9. Each local policy on the use of surveillance cameras and the management of surveillance camera data must include the following details:

[5] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

[6] https://www.gov.uk/government/organisations/home-office/about/personal-information-charter

[7] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool

- why the data is needed and how it will be processed
- what processes are in place to avoid collecting too much or irrelevant information
- any restrictions on access to data and other security measures for maintaining the security of the footage
- the procedures for sharing data with other organisations
- the procedures for notifying detainees and visitors that surveillance cameras systems are in use, and why they are deemed necessary – including the use of surveillance systems during the removal process
- data retention periods and deletion processes - in accordance with paragraphs 38-51.
- audit and assurance processes in connection with the use of surveillance cameras must include the completion and recording of quarterly audits to ensure that information held, both personal and procedural, can be accounted for.

10. Centre suppliers must inform detainees on induction into the centre that there is surveillance camera equipment in operation within the establishment, and explain the circumstances in which each type of equipment is used.

11. Internal and external signage should be displayed at each entrance to the centre notifying detainees and visitors that surveillance cameras are in use and visual and audio recording may be carried out. Internal notices should also detail the process for accessing material for those subject to surveillance, including an IRC supplier contact telephone number for detainees to use in case of query or complaint.

12. Surveillance cameras should not be used in toilets, showers, bedrooms, prayer rooms, healthcare facilities or rooms or areas primarily used for the searching of persons, unless there are exceptional circumstances (e.g. first responders to a serious incident) and their use is strictly necessary in order to gather evidence, and there is no other reasonable means of gathering the necessary evidence. In these cases their use should be authorised by the duty manager and the justification recorded in writing in local supplier records.

13. If it is not possible to get duty manager authorisation the member of staff recording the incident should state out loud the justification for its use in these areas to the camera, so that there is a formal record of the decision.

14. Cameras may be used by staff to record briefing or debriefing sessions before or following an incident. Recorded briefings must never be a replacement for written statements or incident reports . The preparation of any briefing or debriefing transcripts does not mean that any recorded footage can be deleted.

15. Where possible all surveillance cameras in use should have a built in memory and the recorded footage should be encrypted.

Body Worn Cameras (BWC)

16. Home Office guidance on body worn cameras can be found here: https://www.gov.uk/government/publications/safeguarding-body-worn-video-bwv-data

17. Centre suppliers must have in place effective procedures to manage BWC assets. These procedures should accurately record who a device is assigned to, the location of the device and its operational status. The procedures used to manage BWC assets must be fully auditable and records of the use of each camera or of each officer assigned to use BWC must be made available to the local HOIE manager or Home Office Security staff on demand.

18. When involved in any incident which would normally cause BWC to be activated (as set out in the local policy) the user should commence recording at the earliest opportunity. The member of staff recording the incident should state out loud the reason for turning on the BWC. This ensures that that there is a formal record of the decision to use the BWC and also notifies detainees and staff in the area that they are being recorded by both video and audio surveillance (if applicable). Staff dressed in personal protective equipment (PPE) should also identify themselves to camera, ensuring that their protective helmets (with numbers) are visible to camera before carrying out any actions. This will ensure that they are identifiable when incidents are reviewed.

19. Recordings should be uninterrupted from the beginning until the end of the incident, unless a lengthy incident occurs where there may be periods of inactivity, in which only relevant parts of the incident may be filmed. The camera user should cease recording when either the incident has concluded or it is no longer felt justifiable, proportionate or necessary to continue to record. The operator must document and justify the decision to stop recording in his written statements or incident reports following the incident. If a request has been made to cease recording it is for the camera operator to decide if this is justifiable or if the recording should continue. Should the operator continue recording, the justification must be stated to the camera. Once the recording has ceased, the data should be downloaded from the device at the end of the shift or earlier if possible.

20. BWCs should be used:

    - When spontaneous use of force is required against a detainee(s);

    - On a planned relocation where the use of force is assessed as a possibility – see also paragraph 23

- If the wearer believes the interaction presents, or is likely to present, a risk to the safety of the wearer, other members of staff, detainee or other persons present
- If the wearer considers the use of BWC to be a necessary and proportionate means of recording any other interaction or event
- When available, consideration should be given by officers to activating a BWC at a detainee's request

21. Where BWCs should routinely be used as per paragraph 20 but have not been used, records must be kept of the reasons why.

22. BWCs must not be used to:

    - Film covertly
    - Record general work practices
    - Record interactions between any persons without specific cause
    - Record the conduct of any type of search of a person.

23. In accordance with DSO 07/2016 ‘Use of restraints’, all use of force paperwork must be completed by each officer, independently of other staff involved. Ideally, reports should be completed as soon as possible after the incident. Failure to do so may leave staff/managers/suppliers open to serious allegations, disciplinary action and possible litigation. Once completed, all use of force paperwork must be submitted to the local Home Office Immigration Manager as soon as possible and no later than 24h following the incident.

24. When surveillance cameras are used to record an incident involving the use of force. The use of force report must contain a log or reference number of the footage in accordance with paragraphs 38-39.

25. BWCs must be stored in a secure location with limited and controlled access – see paragraphs 36-49. There must be a process in place to account for BWCs on a daily basis to prevent the loss of data and to ensure that they are in good working order. Each centre must have a nominated BWC system administrator who is responsible for ensuring that all BWC are accounted for on a daily basis and that any footage is fully downloaded.

Hand Held Cameras (HHC)

26. For security and audit purposes, BWC should be used in preference to HHC. However, there will be certain circumstances when HHC should be used alongside, or instead of BWC. HHC may provide better quality footage than BWC during a planned

relocation incident where the use of force is assessed as a possibility . In these cases, HHC with built in memory can be used.

27. HHCs must not be used to:

    - Film covertly
    - Record general work practices
    - Record interactions between any persons without specific cause
    - Record the conduct of any type of search of a person.

28. If the HHC records audio, the guidance on staff identifying themselves to camera detailed at paragraph 16 should be followed.

29. Centre suppliers must ensure that there is a process in place to account for HHCs on a daily basis to prevent the loss of data and to ensure that they are in good working order. Once the recording has ceased, the data should be downloaded from the device at the earliest possible opportunity and within a maximum of 8 hours and stored in accordance with paragraphs 38-48.

Closed Circuit Television (CCTV)

30. Where CCTV is installed, it should only be used for official purposes and to meet the following needs:

    - Prevent escape
    - Detect threats to safety and security
    - Detect crime
    - Monitor the movement of vehicles and people through secure areas

31. Particular attention should be given to the location of these cameras to ensure that they fulfil these purposes and do not capture excessive or irrelevant personal data.

32. As a minimum suppliers must undertake daily checks of their CCTV systems and records of these checks should be maintained. Any errors within the system, for example a camera not working, should be reported to a supplier manager as soon as possible. Any **critical** failures of any CCTV system for a significant period of time or where a significant area under surveillance cannot be monitored, must be reported to the local HOIE Immigration Manager, or on-call manager if out of hours, as soon as possible

Escort Vehicles

33. There must be a policy in place which details the requirements and use of surveillance cameras during escorts undertaken by the escort supplier using vehicles fitted with surveillance cameras. The recording equipment within vehicles and any recorded footage should be treated in accordance with the requirements set out in this order.

34. Notices should be displayed within all escort vehicles notifying those in the vehicle that surveillance cameras are in use. The notices should also detail the process for those subject to surveillance to access material, including an escort or centre supplier contact telephone number for detainees to use in case of query or complaint.

35. For any incident involving the use of force, or the use of restraints during escort, all relevant use of force paperwork must be completed and submitted to the Home Office use of force monitor. DSO 07/2016 ‘use of restraints for escorted moves’ provides further guidance on the use of restraints on detainees under escort.

Targeted Surveillance

36. If a surveillance camera is used to actively monitor an individual or group, whether inside or outside the IRC (for example during a protest) it should be conducted in accordance with the procedures set out in DSO 02/2015, Regulation of Investigatory Powers Act 2000 (RIPA). Once directed surveillance is considered operationally necessary by the IRC centre manager, an SV1 application form detailing the need for surveillance should be completed by a member of the IRC security team (the applicant) sent to the Home Office. RIPA (or RIPSA in Scotland) authorisation should be gained beforehand and if this is not possible, retrospective authorisation is required.

37. RIPA/RIPSA provides a framework to ensure investigatory techniques are used in a way that is compatible with the Article 8 right to respect for private and family life, enshrined in the European Convention on Human Rights (ECHR). RIPA/RIPSA ensures that these techniques are used in a regulated way and provides safeguards against the abuse of such methods. Use of these covert techniques will only be authorised if considered legal, necessary and proportionate.

Storage and retention of footage

38. Under the Data Protection Act 1998, those operating surveillance camera systems or who use or process images and information obtained by such systems must have a clearly defined policy to control how images and information are stored and who has access to them.

39. Irrespective of any potential criminal procedures. The inappropriate access, deletion or alteration of any records obtained from surveillance camera systems for which the

Home Office is the data controller constitutes a breach of security and can lead to the suspension or revocation of the Home Office certification of custodial staff, or disciplinary action against Home Office staff.

40. All stored surveillance camera footage must be classified as Official-Sensitive under the government security classifications. Stored camera footage and all communications containing such footage must contain the following handling instructions:

    OFFICIAL SENSITIVE - Contains personal sensitive information, subject to confidentiality requirements under the Data Protection Act. Do not circulate this information further without prior approval from [insert details of local Information Security Manager].

41. Surveillance camera footage should, where possible, be stored on encrypted memory cards or hard drives and held in a locked cupboard. Access to this area must be restricted to reduce the risk of data loss and/or unauthorised access to footage.

42. A record should be kept as an audit trail of how images and information are handled including details on who accessed them (for example police, supplier, Home Office), when and why. Access to footage should be restricted and no footage must be viewed without a justifiable reason, which must be documented within the audit trail. This audit trail must be available to the local HOIE manager on request and will be subject to ad hoc reviews by the Home Office.

43. Data should be stored using a reference number and must not include the details of individuals on the footage within the file name. The names of the subjects on the footage should be held separately and should include the reference number of the footage.

44. If surveillance camera footage is not stored on encrypted removable media and locked in a secure location, BWC/HHC material must be uploaded onto the data processor's IT system as soon as practically possible, in order to ensure that the data is securely saved. Once uploaded the centre supplier duty manager must decide if the footage is either non-evidential or evidential (likely to be required at a future point as evidence such as use of force) and then mark the material accordingly. This marking should include the time, date and a reference number.

45. Evidential footage may include footage of events before and after an incident. It may also include the recording of events where an incident hasn't occurred, for example, the preparatory actions of a planned relocation of a detainee where use of force is assessed as a possibility may in themselves constitute evidential footage.

46. All non-evidential surveillance camera footage must be retained for a minimum of 120 days. This retention period is important because there may be occasions that a detainee, staff member or visitor makes a complaint about an incident and retaining the footage for this length of time (the period in which a complaint can be made as set

out in DSO 03/2015 ‘handling of complaints’) will ensure that it is available to view in these circumstances. If a complaint is made, any relevant footage previously classed as non-evidential must be retained in line with evidential footage retention periods (see paragraph 46).

47. All evidential footage (use of force, assault or any other serious incident) must be retained for a minimum of 6 years to ensure it is available in case of litigation. If footage has been marked as ‘evidential footage’ it must be transferred to an encrypted memory stick or hard drive and stored in a locked cupboard with access restricted.

48. At least once a month the centre supplier security manager must review 5% of the month’s recordings to ensure that the use of the camera was justified, the quality of the recording is sufficient and that it is being retained and tagged appropriately. Any footage that raises concerns or records an incident that had not been previously identified must be escalated appropriately. Auditable records of these checks must be maintained and be available to the Home Office on request.

Deleting footage

49. If the footage has been transferred onto an encrypted memory card or hard drive this should then be deleted from the IT system. Once the memory card or hard drive has passed its retention date and is no longer needed the footage should then be deleted so that the memory card or hard drive can be re-used.

50. The centre supplier must ensure that when footage is deleted it is removed from any computer systems in its entirety. It’s recommended that the software used for deletion of footage complies with HMG infosec standard No.5[8].

51. An audit trail should be available for all historical footage demonstrating the history of the data from filming to storage, subsequent access and deletion.

Access to footage

52. A system operator should have clear polices and guidelines in place to deal with any requests that are received. A data audit trail recording what footage has been reviewed, by who and the reasons why must be kept for every occasion footage is accessed. This should include when the footage has been reviewed for the purposes of quality control. The audit trail should be made available to Home Office managers on request. Judgements about the disclosure of material should be made by Home Office (as data controller) who has the discretion to refuse any request for information unless there is an overriding legal obligation, such as a court order or information access rights, with input from the centre supplier (as data processor). In case of query

[8] https://www.ncsc.gov.uk/guidance/information-risk-management-gpg-47

the centre supplier should approach their local Home Office Immigration Enforcement Delivery Manager for advice.

53. All footage must be made available to the Home Office within 24 hours of a request. Centre Managers, or any senior manager given the authority to do so, may access surveillance camera material where there is a clear and justifiable need to do so.

54. Footage may also be requested by other organisations or departments, for example other government departments and agencies; local authorities; police and other law enforcement agencies, courts and other judicial bodies, Her Majesty's Inspectorate of Prisons or the Prison or Probation Ombudsman. These requests should be sent to the data processor via email, including the reason for the request and should be responded to within 48 hours. If access is granted, the data should be made available within an additional 72 hours. The Home Office should be notified of all such requests and, where material is provided, this should be done on an encrypted memory card.

55. If a detainee requests a copy of the data that is being held about them they must apply in writing to the Home Office via the Personal Information Charter on the Home Office page of GOV.UK (Personal Information Charter). On receipt the Home Office team will discuss the request with the HOME Office IE Delivery Manager and centre supplier. If the Home Office is obliged to answer the request the centre supplier (as data processor) must provide the information to the Home Office as soon as possible, and at the latest within 30 days, to ensure that the Home Office is able to respond to the request within the 40 day time limit as set out in the Data Protection Act.

56. If a centre supplier or the Home Office receives a subject access request (SAR) to disclose surveillance images of individuals the footage must be reviewed by the supplier to establish whether the identifying features of any of the other individuals in the image (whether detainees or staff) need to be obscured. If the Home Office central information team agree it is appropriate to disclose the information arrangements will be made by the Home Office, in conjunction with the supplier, for ensuring that any third party images are obscured, whether undertaken in-house or by another organisation.

57. All requests for access to data must be formally recorded by the supplier for audit purposes.

58. Healthcare staff must not use body worn or hand held cameras. The use of CCTV in healthcare areas in England should only be undertaken with the authority of NHS England who is the data controller in these circumstances. In these circumstances information on the relevant NHS England contact for data access should be displayed in the centre and a local policy must be in place for their use.

Training

51. All IRC supplier staff who use surveillance cameras or manage surveillance camera data should have a good understanding of the legislation controlling its use and should be trained on the operation of the equipment. The training should also include:

    - The circumstances in which BWC or HHC can be used (see paragraphs 16-26)
    - Diversity issues and the provisions of ECHR
    - When to commence and cease recording
    - The importance of identifying recordings for retention or deletion

59. The local policy and procedures should be included in initial training courses for all staff and should be refreshed on an annual basis, which should include regular reviews to develop practice.